UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/448,154	11/24/1999	PAUL S. GERMSCHEID	33012/274/10	4721

27516 7590 02/23/2006

UNISYS CORPORATION
MS 4773
PO BOX 64942
ST. PAUL, MN 55164-0942

EXAMINER	
WASSUM, LUKE S	

ART UNIT	PAPER NUMBER
2167	

DATE MAILED: 02/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/448,154	GERMSCHEID ET AL.	
	Examiner	Art Unit	
	Luke S. Wassum	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 April 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The Applicants' amendment, filed 17 January 2006, has been received, entered into the record, and considered.

2. As a result of the amendment, claims 1, 6, 11 and 16 have been amended. Claims 1-20 remain pending in the application.

The Invention

3. The claimed invention is an apparatus for and method of using an Internet terminal coupled to the World Wide Web to access an existing proprietary database management system, wherein said accessing does not require the transmission of a user identifier across the Internet, thereby enhancing security. Sign in information from a user (such as a user id and password) is processed only at the Internet terminal, and only a special field indicative of the site specific user validation data is transmitted over the Internet as part of the service request.

Specification

4. Applicant has incorporated by reference numerous co-pending applications at various points in the specification. Examiner notes that incorporation by reference of an application in a printed United States Patent constitutes a special circumstance under 35 U.S.C. § 122 warranting that access of the original disclosure of the application be granted. The incorporation by reference will be interpreted as a waiver of confidentiality of only the original disclosure as filed, and not the entire application file. See *In re Gallo*, 231 USPQ 496 (Comm'r Pat. 1986).

If Applicant objects to access to the entire application file(s), two copies of the information incorporated by reference must be submitted along with the objection. Failure to provide the material within the period provided will result in the entire application(s) (including prosecution) being made available to petitioner. The Office will not attempt to separate the noted materials from the remainder of the application. See *In re Marsh Engineering Co.*, 1913 C.D. 183 (Comm'r Pat. 1913).

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

7. Regarding claims 1, 6, 11 and 16, the newly added limitations (the hidden field containing a constant indicative of a site specific identifier) is not disclosed in the originally-filed specification, claims, and drawings. This is a new matter rejection.

See *In re Rasmussen*, 650 F.2d 1212, 211 USPQ 323 (CCPA 1981).

8. Claims 2-5, 7-10, 12-15 and 17-20, fully incorporating the deficiencies of their respective parent claims, are likewise rejected.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

11. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made

in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

12. Claims 1-4, 6-8, 11-14 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") in view of **Steele et al.** (U.S. Patent 6,282,175).

13. Regarding claim 1, **Garrison** teaches a data processing environment having a user with a user identifier which uniquely identifies said user at a terminal at a particular site and wherein said user utilizes said terminal to generate a particular one of a plurality of service requests requesting access to secure data responsively coupled via a publicly accessible digital data communication network to a database management system having at least one database containing said secure data as claimed, comprising a security profile whereby said database management system permits said terminal to access said at least one database (see col. 4, lines 1-32; see also col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach a data processing environment wherein the user accesses the database by transferring a second user identifier which uniquely identifies a particular site without transfer of said user identifier via said publicly accessible digital data communication network, nor including an administration module located within said database management system

for permitting a manager having authority to access said administration module to associate a particular security level with each of said plurality of service requests.

De Capitani di Vimercati et al., however, teaches a data processing environment wherein the user accesses the database by transferring a second user identifier having a hidden field containing a constant indicative of a site specific identifier which uniquely identifies a particular site without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access),

and furthermore including an administration module located within said database management system for permitting a manager having authority to access said administration module to associate a particular security level with each of said plurality of service requests (see extensive discussion of the administration of authorizations, sections 2.3 Administration of Authorizations, page 90, and 2.4 Authorization Specification, page 91, and particularly the following disclosures: "The federation administrator specifies authorizations to access the federated objects and the access control decision is taken only with respect to these authorizations", page 90, col. 2, last paragraph; "...access control decisions are taken only with respect to authorizations specified by the local administrator", page 90, col. 2, last sentence, continuing onto page 91; "The federated administrator specifies global authorizations to access the federated data [and t]he local administrator specifies authorizations to access the local objects", page 91, col. 1, second paragraph under section 2.4), access furthermore being permitted if said second user identifier has said hidden field containing said constant indicative of said site specific identifier (see disclosure that access control at the

federation is enforced on the basis of the site where the connection originated, page 88, col. 2, last paragraph).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network (i.e., global authentication), since the alternative would be to impose local authentication, wherein users are required to re-authenticate themselves at each local site, which may make the access control process very heavy (see **De Capitani di Vimercati et al.**, page 89, col. 2, last paragraph through page 90, col. 1, first paragraph).

Finally, it would have been obvious to one of ordinary skill in the art at the time of the invention to provide a mechanism to allow an administrator to configure the requirements for authorization to specific objects in the database by system users, since without such a mechanism all objects would necessarily have the same level of access, there being no mechanism to change said level of access.

Neither **Garrison** nor **De Capitani di Vimercati et al.** explicitly teaches a data processing environment wherein said service request is honored by executing a sequence of command language scripts having an associated security profile.

Steele et al., however, teaches a data processing environment wherein a service request is honored by executing a sequence of command language scripts having an associated security profile (see col. 4, line 57 through col. 5, line 4; see also col. 7, lines 33-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to satisfy service requests through the execution of command language scripts having an associated security profile, since upon receipt of the service request the request can be satisfied merely by executing the corresponding predefined command language script (see **Steele et al.**, col. 7, lines 33-56), without the necessity to first translate the request into a valid SQL command and then submit the SQL command to the database (as is the case in **Garrison**, col. 8, lines 9-19).

14. Regarding claim 6, **Garrison** teaches an apparatus as claimed, comprising:

a) a terminal located at a particular location (see col. 4, lines 1-32) having a user with a user identifier which identifies said user (see col. 6, line 60 through col. 7, line 13) and generates a particular one of a plurality of service requests (see col. 7, lines 25-32);

b) a database management system having access to a database responsively coupled to said user terminal via a publicly accessible digital data communication network (see col. 4, lines 1-32) and honors said particular one of said plurality of service requests (see col. 7, lines 50-67); and

c) a security profile generated by said database management system whereby said database management system provides access to a particular secure portion of said database corresponding to said security profile (see col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach an apparatus wherein the user accesses the database by transferring a second user identifier which uniquely identifies a particular site without transfer of said user identifier via said publicly accessible digital data communication network, nor including an administration module located within said database management system for permitting a manager having authority to access said administration module to associate a particular security level with each of said plurality of service requests.

De Capitani di Vimercati et al., however, teaches an apparatus wherein the user accesses the database by transferring a second user identifier having a hidden field containing a constant indicative of a site specific identifier which uniquely identifies a particular site without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access),

and furthermore including an administration module located within said database management system for permitting a manager having authority to access said administration module to associate a particular security level with each of said plurality of service requests (see extensive discussion of the administration of authorizations, sections 2.3 Administration of Authorizations, page 90, and 2.4 Authorization Specification, page 91, and particularly the following disclosures:

"The federation administrator specifies authorizations to access the federated objects and the access control decision is taken only with respect to these authorizations", page 90, col. 2, last paragraph; "...access control decisions are taken only with respect to authorizations specified by the local administrator", page 90, col. 2, last sentence, continuing onto page 91; "The federated administrator specifies global authorizations to access the federated data [and t]he local administrator specifies authorizations to access the local objects", page 91, col. 1, second paragraph under section 2.4), access furthermore being permitted if said second user identifier has said hidden field containing said constant indicative of said site specific identifier (see disclosure that access control at the federation is enforced on the basis of the site where the connection originated, page 88, col. 2, last paragraph).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network (i.e., global authentication), since the alternative would be to impose local authentication, wherein users are required to re-authenticate themselves at each local site, which may make the access control process very heavy (see **De Capitani di Vimercati et al.**, page 89, col. 2, last paragraph through page 90, col. 1, first paragraph).

Finally, it would have been obvious to one of ordinary skill in the art at the time of the invention to provide a mechanism to allow an administrator to configure the requirements for authorization to specific objects in the database by system users, since without such a mechanism all objects would necessarily have the same level of access, there being no mechanism to change said level of access.

Neither **Garrison** nor **De Capitani di Vimercati et al.** explicitly teaches an apparatus wherein said service request is honored by executing a sequence of command language scripts having an associated security profile.

Steele et al., however, teaches an apparatus wherein a service request is honored by executing a sequence of command language scripts having an associated security profile (see col. 4, line 57 through col. 5, line 4; see also col. 7, lines 33-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to satisfy service requests through the execution of command language scripts having an associated security profile, since upon receipt of the service request the request can be satisfied merely by executing the corresponding predefined command language script (see **Steele et al.**, col. 7, lines 33-56), without the necessity to first translate the request into a valid SQL command and then submit the SQL command to the database (as is the case in **Garrison**, col. 8, lines 9-19).

15. Regarding claim 11, **Garrison** teaches a method of utilizing a user terminal having a first identifier and a user with a user identifier located at a site to securely access a remote database management system having a database via a publicly accessible digital data communication network as claimed, comprising:

a) signing on to said terminal by said user utilizing said user identifier (see col. 2, line 64 through col. 3, line 2, disclosing that the client transmits a password to the client to identify the user of the client system, meaning that the user has necessarily signed on to the client system utilizing a user identifier);

b) transmitting a service request requiring secure access to said database from said terminal (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

c) receiving said service request by said remote database management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

d) determining a security profile (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

e) comparing said security profile with said first identifier (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and

f) honoring said service request if and only if said first identifier corresponds to said security profile (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach a method wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network, nor

including an administration module located within said database management system for permitting a manager having authority to access said administration module to associate a particular security level with each of said plurality of service requests.

De Capitani di Vimercati et al., however, teaches a method wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access),

including the transmission of a request of a first identifier from said user terminal (see disclosure on page 89, col. 2, last paragraph, that "Upon reception of the requests by the federation..."), the user identifier having a hidden field containing a constant indicative of a site specific identifier (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access),

and furthermore including an administration module located within said database management system for permitting a manager having authority to access said administration module to associate a particular security level with each of said plurality of service requests (see extensive discussion of the administration of authorizations, sections 2.3 Administration of Authorizations, page 90, and 2.4 Authorization Specification, page 91, and particularly the following disclosures: "The federation administrator specifies authorizations to access the federated objects and the access control decision is taken only with respect to these authorizations", page 90, col. 2, last paragraph; "...access control decisions are taken only with respect to authorizations specified by the local

administrator", page 90, col. 2, last sentence, continuing onto page 91; "The federated administrator specifies global authorizations to access the federated data [and t]he local administrator specifies authorizations to access the local objects", page 91, col. 1, second paragraph under section 2.4).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network (i.e., global authentication), since the alternative would be to impose local authentication, wherein users are required to re-authenticate themselves at each local site, which may make the access control process very heavy (see **De Capitani di Vimercati et al.**, page 89, col. 2, last paragraph through page 90, col. 1, first paragraph).

Finally, it would have been obvious to one of ordinary skill in the art at the time of the invention to provide a mechanism to allow an administrator to configure the requirements for authorization to specific objects in the database by system users, since without such a mechanism all objects would necessarily have the same level of access, there being no mechanism to change said level of access.

De Capitani di Vimercati et al. additionally teaches alternative authentication wherein a request is transmitted to the database without any identifier, necessitating the database subsequently transmitting a request for an identifier to be used for authentication (see page 89, last paragraph).

Given the teaching of a system wherein authentication information is transmitted together with a database request, it would have been an obvious variant to transmit the authentication information and database request separately, since this would conserve bandwidth in cases where some database requests could be serviced without authentication.

Neither **Garrison** nor **De Capitani di Vimercati et al.** explicitly teaches a method wherein said service request is honored by executing a sequence of command language scripts having an associated security profile.

Steele et al., however, teaches a method wherein a service request is honored by executing a sequence of command language scripts having an associated security profile (see col. 4, line 57 through col. 5, line 4; see also col. 7, lines 33-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to satisfy service requests through the execution of command language scripts having an associated security profile, since upon receipt of the service request the request can be satisfied merely by executing the corresponding predefined command language script (see **Steele et al.**, col. 7, lines 33-56), without the necessity to first translate the request into a valid SQL command and then submit the SQL command to the database (as is the case in **Garrison**, col. 8, lines 9-19).

16. Regarding claim 16, **Garrison** teaches an apparatus as claimed, comprising:

a) permitting means located at a site having a first identifier for permitting a user having a user identifier to interact with a database responsively coupled via a publicly accessible digital data communication network (see col. 4, lines 1-32);

b) means responsively coupled to said permitting means via said publicly accessible digital data communication network for offering data processing services involving access to said database in response to said service request (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and

c) means responsively coupled to said offering means for preventing said offering means from offering said data processing services to said user in response to said service request unless said site corresponds to a security profile wherein said security profile permits access to said database (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37), wherein the existence of the security profile renders the claimed administration module inherent, since the only claimed functionality if the administration module is to maintain the security profile, and the reference teaches the maintenance of a security profile at col. 7, lines 50-67 and col. 10, lines 5-17.

Garrison does not explicitly teach an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network, nor including an administration module located within said database management system for permitting a manager having authority to access said administration module to associate a particular security level with each of said plurality of service requests.

De Capitani di Vimercati et al., however, teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access), the user identifier having a hidden field containing a constant indicative of a site specific identifier (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access),

and furthermore including a means for permitting a manager having authority to access said administration module to associate a particular security level with each of said plurality of service requests (see extensive discussion of the administration of authorizations, sections 2.3 Administration of Authorizations, page 90, and 2.4 Authorization Specification, page 91, and particularly the following disclosures: "The federation administrator specifies authorizations to access the federated objects and the access control decision is taken only with respect to these authorizations", page 90, col. 2, last paragraph; "...access control decisions are taken only with respect to authorizations specified by the local administrator", page 90, col. 2, last sentence, continuing onto page 91; "The federated administrator specifies global authorizations to access the federated data [and t]he local administrator specifies authorizations to access the local objects", page 91, col. 1, second paragraph under section 2.4).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the references, since they are all concerned with the same field of endeavor, that is,

remotely accessing databases (see **Garrison**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network (i.e., global authentication), since the alternative would be to impose local authentication, wherein users are required to re-authenticate themselves at each local site, which may make the access control process very heavy (see **De Capitani di Vimercati et al.**, page 89, col. 2, last paragraph through page 90, col. 1, first paragraph).

Finally, it would have been obvious to one of ordinary skill in the art at the time of the invention to provide a mechanism to allow an administrator to configure the requirements for authorization to specific objects in the database by system users, since without such a mechanism all objects would necessarily have the same level of access, there being no mechanism to change said level of access.

Neither **Garrison** nor **De Capitani di Vimercati et al.** explicitly teaches an apparatus wherein said service request is honored by executing a sequence of command language scripts having an associated security profile.

Steele et al., however, teaches an apparatus wherein a service request is honored by executing a sequence of command language scripts having an associated security profile (see col. 4, line 57 through col. 5, line 4; see also col. 7, lines 33-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to satisfy service requests through the execution of command language scripts having an associated security profile, since upon receipt of the service request the request can be satisfied merely by executing the corresponding predefined command language script (see **Steele et al.**, col. 7, lines 33-56), without the necessity to first translate the request into a valid SQL command and then submit the SQL command to the database (as is the case in **Garrison**, col. 8, lines 9-19).

17. Regarding claims 2 and 13, **De Capitani di Vimercati et al.** additionally teaches a data processing environment wherein a security profile is generated by said data management system (see sections 2.3 Administration of Authorizations, page 90, and 2.4 Authorizations Specification, page 91, disclosing the specification by the federation administrator of authorizations to access federated data, and particularly the following disclosures: "The federation administrator specifies authorizations to access the federated objects and the access control decision is taken only with respect to these authorizations", page 90, col. 2, last paragraph; "...access control decisions are taken only with respect to authorizations specified by the local administrator", page 90, col. 2, last sentence, continuing onto page 91; "The federated administrator specifies global authorizations to access the federated data [and t]he local administrator specifies authorizations to access the local objects", page 91, col. 1, second paragraph under section 2.4; see also disclosure that "Federated systems represent one of the new emerging technology for distributed database management and organization", under section 5 Conclusion, page 95).

18. Regarding claims 3, 8, 12 and 18, **De Capitani di Vimercati et al.** additionally teaches an improvement, method and apparatus further comprising a portion of a user identifier whereby said database management system receives an identifier corresponding to said particular site (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access through the use of an identifier corresponding to the site, and not an identifier corresponding to the user).

19. Regarding claims 4, 14 and 17, **Garrison** additionally teaches an improvement, method and apparatus wherein said publicly accessible digital data communication network further comprises the Internet (see col. 4, lines 1-32).

20. Regarding claim 7, **Garrison** additionally teaches an apparatus wherein said terminal accesses said data entity by transferring said one of a plurality of service requests to said system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

21. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") in view of **Steele et al.** (U.S. Patent 6,282,175) as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **Unisys** ("UNISYS CSG MarketPlace – The Mapper System").

22. Regarding claims 5 and 19, **Garrison, De Capitani di Vimercati et al.** and **Steele et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, De Capitani di Vimercati et al.** nor **Steele et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is a legacy database management system.

However, **Unisys** teaches the database management system MAPPER, constituting a legacy database management system (see entire document).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER contains many key features that make its use advantageous for users (see **Unisys**, key features under MAPPER Overview, page 3).

23. Regarding claims 9 and 15, **Garrison, De Capitani di Vimercati et al.** and **Steele et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, De Capitani di Vimercati et al.** nor **Steele et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **Unisys** teaches the database management system MAPPER (see entire document).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER contains many key features that make its use advantageous for users (see **Unisys**, key features under MAPPER Overview, page 3).

24. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

25. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

Response to Arguments

26. Applicant's arguments filed 17 January 2006 have been fully considered but they are not persuasive.

27. Regarding the Applicants' argument that the newly added limitations are supported "throughout the specification and drawings, with particularly detailed disclosure given n Fig. 14, along with accompanying discussion in the specification", the examiner respectfully disagrees.

The new limitation cites a hidden field containing a constant indicative of a site specific identifier. The examiner has been unable to find any supporting disclosure in the specification or drawings.

With respect to Figure 14, the examiner was unable to find any indication of a hidden field, nor any field indicative of a site specific identifier. Furthermore, the accompanying discussion of Figure 14 in the specification, consists in its entirety of the following: "Fig. 14 is a listing of the messages associated with creation of a site security profile." The examiner can find no support for the new limitations in this disclosure.

As a result, all claims have been rejected under U.S.C. § 112, first paragraph, as containing new matter.

28. Regarding the Applicants' arguments that the references are not properly combinable, these arguments have been presented in the Applicants' previous response, and have been answered in the previous Office action.

29. Regarding the Applicants' argument that the **Garrison** reference fails to teach a service request, the examiner respectfully responds that the reference need not use identical terminology to that used by the Applicants. The term 'service request' could be any request for access to a system of data thereon, a limitation clearly taught by the **Garrison** reference, *at least* at col. 7, lines 26-28 "the client is configured to encrypt a request for data using the new encryption key and to transmit the encrypted request for data to the server."

Conclusion

30. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

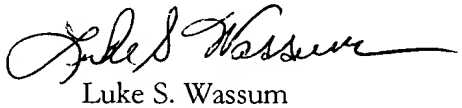
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luke S. Wassum whose telephone number is 571-272-4119. The examiner can normally be reached on Monday-Friday 8:30-5:30, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jean R. Homere can be reached on 571-272-3780. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

In addition, INFORMAL or DRAFT communications may be faxed directly to the examiner at 571-273-4119. Such communications must be clearly marked as INFORMAL, DRAFT or UNOFFICIAL.

Customer Service for Tech Center 2100 can be reached during regular business hours at (571) 272-2100, or fax (571) 273-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Luke S. Wassum
Primary Examiner
Art Unit 2167

lsw
21 February 2006